36e Année (1975-1976) Septembre 1975 N° 1



REVUE DE MATHÉMATIQUES SPÉCIALES

Sujets donnés aux concours d'Agrégation et aux concours d'entrée aux grandes Écoles en 1975

N.D.L.R. — Les sujets des concours, dont nous présentons un éventail aussi large que possible, devenant chaque année plus copieux, nous avons été dans l'obligation de les faire paraître sur deux numéros. Nos lecteurs trouveront donc la suite des sujets au début du numéro deux de la Revue.

AGRÉGATION DES SCIENCES MATHÉMATIQUES 75

Composition de mathématiques générales.

PREMIÈRE PARTIE.

6093. n étant un élément de $\mathbf{N}^*$ (entier naturel non nul), on note $(\pi_1, \pi_2, \ldots, \pi_n)$ la base canonique de l'espace vectoriel $\mathbf{Q}^n$. La matrice d'une forme quadratique $\overline{q}$ relative à cette base est appelée matrice canonique de $\overline{q}$; $\overline{q}$ est dite positive si $\overline{q}(x) \geqslant 0$ pour tout x.

$\mathrm{M}_n(\mathbf{Q})$ (resp. $\mathrm{M}_n(\mathbf{Z})$) est l'algèbre des matrices carrées d'ordre n à coefficients dans $\mathbf{Q}$ (resp. $\mathbf{Z}$). $\mathrm{GL}_n(\mathbf{Q})$ (resp. $\mathrm{GL}_n(\mathbf{Z})$) est le groupe multiplicatif des matrices inversibles de $\mathrm{M}_n(\mathbf{Q})$ (resp. inversibles de $\mathrm{M}_n(\mathbf{Z})$). I est la matrice unité de $\mathrm{M}_n(\mathbf{Q})$. ${}^t\mathrm{M}$ (resp. det M) est la transposée (resp. le déterminant) de la matrice M. Dans cette première partie, n ne prend que les valeurs 2 et 3.

I. — 1° Soit $\overline{q}$ une forme quadratique de $\mathbf{Q}^2$, de matrice canonique $\mathrm{M} = \begin{bmatrix} u & v \\ v & w \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z})$. On pose $\delta = \det \mathrm{M}$. Montrer que, si $\overline{q}$ est non dégénérée, positive, alors $\delta = 1$.

I. — 2° On suppose toujours $\mathrm{M} \in \mathrm{GL}_2(\mathbf{Z})$ et, pour cette question et la suivante, $\delta = 1$. Montrer que l'une des deux formes $\overline{q}$ ou $-\overline{q}$ est non dégénérée, positive.

I. — 3° *a*) En admettant ici que $\overline{q}$ est non dégénérée, positive, démontrer, pour $u \neq 1$, l'existence d'une matrice $\mathrm{P} = \begin{bmatrix} -s & 1 \\ 1 & 0 \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z})$ telle que, si $\mathrm{M}' = {}^t\mathrm{PMP} = \begin{bmatrix} u' & v' \\ v' & w' \end{bmatrix}$, alors $0 < u' \leqslant \frac{u}{2}$.

b) En déduire l'existence de $\mathrm{N} \in \mathrm{GL}_2(\mathbf{Z})$ telle que $\mathrm{M} = {}^t\mathrm{NN}$. Énoncer une propriété relative à la décomposition de $\overline{q}$ en somme de deux carrés.

I. — 4° Jusqu'à la fin de cette première partie, $\overline{q}$ désigne une forme quadratique de $\mathbf{Q}^3$, non dégénérée, positive, dont la matrice canonique

$$\mathrm{M} = \begin{bmatrix} m & p & q \\ p & m' & r \\ q & r & m'' \end{bmatrix}$$

est un élément de $\mathrm{GL}_3(\mathbf{Z})$.

Que peut-on dire des signes de m, m', m'' et $\det M$?
Montrer que, si M n'est pas égale à I, l'une des six inégalités suivantes est vérifiée :

$$|p| > \frac{m}{2}, \quad |p| > \frac{m'}{2}, \quad |q| > \frac{m}{2}, \quad |q| > \frac{m''}{2}, \quad |r| > \frac{m'}{2}, \quad |r| > \frac{m''}{2}.$$

(On pourra séparer le cas $m = m' = m''$, puis le cas $m \geqslant m' \geqslant m''$, $m > m''$.)

I. — 5° *a*) Déterminer alors une matrice triangulaire $P \in GL_3(\mathbf{Z})$ telle que $M_1 = {}^tPMP$ soit de même type que M, avec, par exemple,

$$m_1 = m, \quad m'_1 \leqslant m' - 1, \quad m''_1 = m''.$$

b) En déduire l'existence de $N \in GL_3(\mathbf{Z})$ telle que $M = {}^tNN$.
Énoncer une propriété relative à la décomposition de $\bar{q}$ en somme de trois carrés.

c) **Application numérique :** $M = \begin{bmatrix} 5 & 0 & 3 \\ 0 & 1 & 1 \\ 3 & 1 & 3 \end{bmatrix}$ (on se limitera à exhiber une matrice N).

I. — 6° Donner un exemple de matrice $M \in GL_3(\mathbf{Z})$, telle que ${}^tM = M$, que $\det M = 1$ et qu'il n'existe aucune matrice $N \in GL_3(\mathbf{Z})$ vérifiant $M = {}^tNN$ (un exemple à coefficients dans $\mathbf{N}^*$ serait apprécié).

I. — 7° Retrouver les résultats de la question **I, 3°** à partir de ceux du **5°**. Comparer les deux méthodes.

Deuxième partie.

V est un espace vectoriel de dimension n sur $\mathbf{Q}$; H, H' ..., sont, par convention, des sous-groupes additifs de V (confondus, selon l'usage, avec les ensembles sous-jacents). $\mathscr{H}_0 = \mathrm{Hom}(H, \mathbf{Z})$ est l'ensemble des morphismes de groupe de H vers **Z**. $\hat{H}$ est le sous-espace vectoriel de V engendré par H. La somme $H + H'$ est le sous-groupe de V engendré par $H \cup H'$. Pour $\lambda \in \mathbf{Q}$, λH est l'image de H par l'homothétie de rapport λ.

Une **Z**-base de H est une famille libre de vecteurs de V telle qu'un vecteur de V appartient à H si, et seulement si, il est combinaison linéaire à coefficients entiers relatifs des vecteurs de la famille. Un réseau est un sous-groupe de V admettant au moins une **Z**-base de cardinal n. L, L', ..., sont, par convention, des réseaux de V. Un sous-réseau est un réseau d'un sous-espace vectoriel de V.

II. — 1° Démontrer que $\hat{L} = V$.

II. — 2° $\mathscr{B} = (e_i)_{1 \leqslant i \leqslant p}$ étant une famille finie de vecteurs de V, on note B la matrice des coordonnées des vecteurs e_i, $(1 \leqslant i \leqslant p)$, dans une base (ω_j), $(1 \leqslant j \leqslant n)$, de V considérée comme fixe dans tout le problème : B est appelée matrice canonique de $\mathscr{B}$. Montrer que, B et B' étant les matrices canoniques d'une **Z**-base $\mathscr{B}$ de L et d'une famille finie $\mathscr{B}'$ de vecteurs de L, $\mathscr{B}'$ est une **Z**-base de L si, et seulement si, il existe $P \in GL_n(\mathbf{Z})$ telle que $B' = BP$. Montrer que le rationnel $\mathrm{vol}\, L = |\det B|$ est indépendant du choix d'une **Z**-base de L.

II. — 3° L' étant un réseau de V, montrer qu'il existe $d \in \mathbf{N}^*$ tel que $dL' \subset L$ et que $d^n \left(\frac{\mathrm{vol}\, L'}{\mathrm{vol}\, L}\right)$ est entier.

II. — 4° H étant un sous-groupe de L non réduit à $\{0\}$, montrer que H est un sous-réseau de V (on pourra, par exemple, considérer une **Z**-base (e_i) de L, rechercher un élément a de $\mathbf{N}^*$, une application coordonnée ψ, un vecteur b tel que $\psi(b) = a$ et utiliser l'endomorphisme θ de H défini par $\theta(x) = x - \frac{\psi(x)}{a} b$.)

II. — 5° Montrer que l'intersection et la somme de deux réseaux de V sont des réseaux.

II. — 6° X et Y étant les matrices canoniques de deux vecteurs x et y de V, on note $(x|y) = {}^tXY$ (produit de x et de y), et $\|x\|^2 = {}^tXX$ (carré de x). Une partie A de V est dite bornée s'il existe un rationnel $\mathscr{A}$ tel que $\|x\|^2 \leqslant \mathscr{A}$ pour tout $x \in A$. Montrer que tout sous-groupe H de V dont l'intersection avec toute partie bornée de V est finie est un sous-réseau de V (on pourra considérer une famille libre maximale

$(h_1, \ldots, h_r)$ de vecteurs de H, la partie Ω de V formée des vecteurs $\sum_{i=1}^{r} \mu_i h_i$, $\mu_i \in \mathbf{Q} \cap [0, 1]$, et associer au vecteur $\sum_{i=1}^{r} \lambda_i h_i$, $\lambda_i \in \mathbf{Q}$, le vecteur $\sum_{i=1}^{r} (\lambda_i - [\lambda_i]) h_i$, où le symbole [ ] représente la partie entière).

Démontrer la réciproque.

Troisième partie.

H étant un sous-groupe de V, on note H_0 l'ensemble des $x \in V$ tels que, pour tout $y \in H$, on ait $(x \mid y) \in \mathbf{Z}$. Un réseau L est dit r-modulaire (resp. unimodulaire) si $L_0 = rL$ (resp. $L_0 = L$); il est dit r-modulaire trivial s'il existe une $\mathbf{Z}$-base (e_i) de L orthogonale (c'est-à-dire vérifiant $(e_i \mid e_j) = 0$ pour $i \neq j$] et telle que $\|e_i\|^2 = \frac{1}{r}$ pour tout i ($\frac{1}{r}$ s'appelle alors le carré de la $\mathbf{Z}$-base; cette dernière est dite orthonormale si $r = 1$). $\mathbf{F}_2$ est le corps à deux éléments.

III. — 1° a) Démontrer que, si L est un réseau de V, $\mathscr{L}_0 = \operatorname{Hom}(L, \mathbf{Z})$ est un réseau d'un certain espace vectoriel W de dimension n sur $\mathbf{Q}$ (on pourra utiliser la famille (e_i^0) de $\mathscr{L}_0$ définie par $e_i^0(e_j) = \delta_{ij}$).

b) Définir un isomorphisme α du groupe L_0 sur $\mathscr{L}_0$, indépendant de tout choix de $\mathbf{Z}$-base de L. En déduire que L_0 est un réseau de V, dont on explicitera une $\mathbf{Z}$-base à partir d'une $\mathbf{Z}$-base de L.

III. — 2° L et L′ étant deux réseaux de V, démontrer les égalités :

$$L_{00} = L, \qquad (L + L')_0 = L_0 \cap L'_0, \qquad (L \cap L')_0 = L_0 + L'_0, \qquad (\operatorname{vol} L)(\operatorname{vol} L_0) = 1.$$

Calculer vol L dans le cas où L est r-modulaire.

III. — 3° On suppose jusqu'à la fin de cette partie que L est un réseau r-modulaire trivial. Montrer que L est r-modulaire, et qu'il existe une « similitude directe » (notion que l'on définira par analogie avec la structure euclidienne de $\mathbf{R}^n$) transformant le réseau fondamental Λ, sous-groupe engendré par la base canonique (ω_i), de V, en L.

III. — 4° a) On note Aut L l'ensemble des morphismes de groupe s de L dans lui-même tels que $(s(x)|s(y)) = (x|y)$ pour tout couple (x, y) de L^2. On considère une $\mathbf{Z}$-base (e_i) de L, orthogonale et de carré $\frac{1}{r}$. A tout élément s de Aut L, on associe la matrice S des coordonnées des vecteurs $e'_i = s(e_i)$ dans la $\mathbf{Z}$-base (e_i). Montrer qu'il existe un élément k de S_n (groupe des permutations de $[1, n]$) et une application ε de $[1, n]$ dans $\{-1, +1\}$ tels que l'élément (i, j) de S s'écrive sous la forme $s_{ij} = \varepsilon(j)\, \delta_{i,k(j)}$. Calculer le cardinal de Aut L.

b) Étudier l'ensemble U des $s \in \operatorname{Aut} L$ auxquels on peut associer une application f de $[1, n]$ dans $\{-1, +1\}$ telle que l'élément (i, j) de S s'écrive $s_{ij} = f(i)\, \delta_{i,j}$; un tel s sera noté s_f. Comparer U et le groupe $(\mathbf{F}_2^n, +)$.

c) Étudier l'ensemble T des $s \in \operatorname{Aut} L$ tels que, $k \in S_n$ étant défini comme en **a)**, l'élément (i, j) de S s'écrive $s_{ij} = \delta_{i,k(j)}$; un tel s sera noté s_k.

Comparer T et le groupe $(S_n, \circ)$.

III. — 5° a) Montrer que tout $s \in \operatorname{Aut} L$ se décompose, de manière unique, sous la forme $s = s_f \circ s_k$, $(s_f, s_k) \in U \times T$.

b) Déterminer un morphisme φ de T dans le groupe Aut U des automorphismes de groupe de U tel que U × T, muni de la loi

$$(s_f, s_k) \square (s_{f'}, s_{k'}) = (s_f \circ \varphi(s_k)(s_{f'}), s_k \circ s_{k'}]$$

soit isomorphe à Aut L, muni de la loi $\circ$.

III. — 6° Déterminer une loi $*$ sur le produit cartésien $\mathbf{F}_2^n \times S_n$ telle qu'il existe un isomorphisme θ de ce produit sur Aut L. Caractériser, par analogie avec φ, un morphisme F de S_n dans le groupe linéaire de dimension n sur $\mathbf{F}_2$, en calculant la matrice de F (k) relative à la base canonique de $\mathbf{F}_2^n$.

Quatrième partie.

On définit dans V les isométries (resp. les rotations), et les groupes matriciels correspondants $O_n(\mathbf{Q})$ (resp. $O_n^+(\mathbf{Q})$) par analogie avec les notions similaires des espaces euclidiens réels. Σ_n est l'ensemble des entiers m de la forme $m = \alpha_1^2 + \cdots + \alpha_n^2$, $\alpha_i \in \mathbf{Z}$.

IV. — 1° Dans toute cette partie, L est un réseau unimodulaire de V. (e_i) étant une **Z**-base quelconque de L, de matrice canonique B, on considère l'automorphisme λ de V de matrice canonique B, et la forme quadratique $\bar{q}$ définie par $\bar{q}(x) = \|\lambda(x)\|^2$. Que peut-on dire de la matrice canonique M de $\bar{q}$; de l'image $\bar{q}(\Lambda)$ du réseau fondamental Λ par $\bar{q}$?

IV. — 2° Dans les questions suivantes (jusqu'à IV, 5° incluse), on suppose $n = 3$. Montrer que $\bar{q}(\Lambda) = \Sigma_3$.

IV. — 3° Démontrer que L est unimodulaire trivial. Caractériser, à l'aide des ensembles $O_3^+(\mathbf{Q})$ et $GL_3(\mathbf{Z})$, les matrices canoniques des **Z**-bases des réseaux unimodulaires de V. Comment obtient-on ces réseaux à partir de Λ?

IV. — 4° Résoudre l'équation matricielle ${}^t KK = {}^t BB$, où $K \in GL_3(\mathbf{Z})$ et B est définie au IV, 1°. Dénombrer les solutions.

IV. — 5° Si L′ est un réseau de V tel que $L' \subset L'_0$, démontrer l'existence d'un réseau unimodulaire trivial L tel que $L' \subset L \subset L'_0$ (on pourra considérer $(\Lambda + L') \cap L'_0$).

IV. — 6° Indiquer brièvement ce que deviennent les questions précédentes pour $n = 2$.

Cinquième partie.

$\mathbf{F}_p$ est le corps à p éléments (p : entier naturel premier). La notation p.g.c.d. (x, y, z) représente le plus grand commun diviseur, nécessairement positif, des entiers (x, y, z).

V. — 1° Démontrer que le triplet $(x, y, z) \in \mathbf{N}^3$ est solution de l'équation

$$xz - y^2 = 1$$

si, et seulement si, il existe $(a, b, c, d) \in \mathbf{Z}^4$ tels que

$$ad - bc = 1, \qquad a^2 + b^2 = x, \qquad 0 \leqslant ac + bd = y, \qquad c^2 + d^2 = z.$$

V. — 2° Démontrer que l'équation $x^2 + 1 = 0$ n'a de solutions dans $\mathbf{F}_p$ que si, et seulement si, $p \in \Sigma_2$. Montrer qu'alors ou bien $p = 2$, ou bien il existe $q \in \mathbf{N}$ tel que $p = 4q + 1$.

V. — 3° S'il existe $q \in \mathbf{N}$ tel que $p = 4q + 1$ soit premier, démontrer (par exemple à l'aide du groupe multiplicatif de $\mathbf{F}_p$) que p divise $[(2q)!]^2 - (p-1)!$ et $[(2q)!]^2 + 1$. En déduire les éléments de Σ_2 qui sont des nombres premiers.

V. — 4° Donner une condition nécessaire et suffisante, portant sur la parité des exposants des diviseurs premiers d'un entier m, pour que $m \in \Sigma_2$. En déduire que, si $\bar{q}$ est la forme quadratique définie en IV, 1°, pour $n = 2$, et si x et y sont des vecteurs de Λ tels que $\bar{q}(y)$ divise $\bar{q}(x)$, il existe alors $z \in \Lambda$ tel que

$$\bar{q}(x) = \bar{q}(y)\bar{q}(z).$$

La propriété analogue serait-elle vraie pour $n = 3$? (Considérer par exemple le nombre 7.)

V. — 5° *a)* Soit m un entier; démontrer que l'équation $x^2 + y^2 = mz^2$ n'a de solution $(x, y, z) \in \mathbf{N}^3$ autre que $(0, 0, 0)$ que si, et seulement si, $m \in \Sigma_2$. Déterminer alors toutes les solutions $(x, y, z) \in \mathbf{Q}^3$.

b) En déduire que l'équation $\begin{vmatrix} 1 & p & q \\ p & 1 & r \\ q & r & 1 \end{vmatrix} = 1$, $(p, q, r) \in \mathbf{Z}^3$ n'admet que la solution $(0, 0, 0)$ (on pourra poser, par exemple, $m = p^2 - 1$).

V. — 6° *a)* Déduire des relations $(x, y, z, t) \in \mathbf{N}^{*4}$, p.g.c.d. $(x, y, z) = 1$, $xz = y^2 + t^2$ que x et tous les diviseurs premiers qui figurent dans x à une puissance impaire appartiennent à Σ_2.

b) Démontrer qu'il existe alors $B' \in GL_2(\mathbf{Q})$, $P \in M_2(\mathbf{Z})$, $N \in GL_2(\mathbf{Z})$ telles que

$$M = \begin{bmatrix} x & y \\ y & z \end{bmatrix} = {}^t B'B' = {}^t(NP)NP.$$

V. — 7° Démontrer que le quadruplet $(x, y, z, t) \in \mathbf{N}^4$ est solution de l'équation $xz = y^2 + t^2$, $t \neq 0$ si, et seulement si, il existe $(a, b, c, d, \delta) \in \mathbf{Z}^5$ tels que

$$x = \delta(a^2 + b^2), \qquad y = \delta(ac + bd), \qquad z = \delta(c^2 + d^2), \qquad t = \delta(ad - bc) \neq 0,$$

δ étant le produit des nombres premiers p de la forme $4q + 3$ figurant dans x avec un exposant impair.

V. — 8° $M = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$ étant une matrice de $GL_2(\mathbf{Q})$, démontrer qu'il existe $A \in M_2(\mathbf{Z})$ telle que $M = {}^tAA$ si, et seulement si, $(x, y, z) \in \mathbf{Z}^3$, $\sqrt{xz - y^2} \in \mathbf{N}^*$, $x \in \Sigma_2$.

Examiner le cas où $M \in M_2(\mathbf{Q})$, $\det M = 0$.

V. — 9° ω appartenant à $\mathbf{Z}$, démontrer que le quadruplet $(x, y, z, t) \in \mathbf{Z}^4$ est solution de l'équation $xz = y^2 + \omega t^2$ si, et seulement si, il existe $(\alpha, \beta, \gamma, \delta, g, p, q) \in \mathbf{Z}^7$ tel que

$$\omega = \alpha\gamma - \beta^2, \qquad x = d(\alpha p^2 + 2\beta pq + \gamma q^2), \qquad y = dg(\beta p + \gamma q), \qquad z = dg^2\gamma, \qquad t = dgp.$$

(On pourra par exemple se ramener au cas où p.g.c.d. $(t, y) = 1$, en posant :

$$d = \text{p.g.c.d.}\,(x, y, z, t), \qquad d\Delta = \text{p.g.c.d.}\,(t, y), \qquad d\delta = \text{p.g.c.d.}\,(d\Delta, x)$$

et en exprimant y en fonction de t et z.)

En déduire que le quadruplet $(x, y, z, t) \in \mathbf{Z}^4$ est solution de l'équation $xz = y^2 + t^2$ si, et seulement si, il existe $(a, b, c, d, \delta) \in \mathbf{Z}^5$ tels que

$$x = \delta(a^2 + b^2), \qquad y = \delta(ac + bd), \qquad z = \delta(c^2 + d^2), \qquad t = \delta(ad - bc).$$

Composition d'analyse.

PRÉAMBULE.

Les propriétés suivantes de la fonction Γ pourront être utilisées sans démonstration; elles n'interviennent pas dans la première partie du problème.

Soit s un nombre complexe; on note $\operatorname{Re}(s)$ sa partie réelle, $\operatorname{Im}(s)$ sa partie imaginaire. Pour $\operatorname{Re}(s) > 0$, on pose $\Gamma(s) = \int_0^{+\infty} e^{-t} t^{s-1}\, dt$.

La fonction Γ est holomorphe dans le demi-plan $\operatorname{Re}(s) > 0$. Elle se prolonge en une fonction méromorphe dans $\mathbf{C}$ dont les pôles sons les entiers négatifs ou nuls. Ces pôles sont simples, et le résidu de Γ au point

$$s = -p, \qquad (p \in \mathbf{N}), \qquad \text{est } \frac{(-1)^p}{p!}.$$

Si s n'est pas un pôle, on a $\Gamma(s + 1) = s\,\Gamma(s)$, et $\Gamma(s) \neq 0$.

Soit σ_1, σ_2 des nombres réels tels que $\sigma_1 \leqslant \sigma_2$, et m un entier positif; on a $\lim_{|t| \to +\infty} |t^m\,\Gamma(\sigma + it)| = 0$, uniformément pour σ élément de $[\sigma_1, \sigma_2]$.

Enfin, si c et x sont des nombres réels strictement positifs, on a

$$e^{-x} = \frac{1}{2i\pi} \int_{\operatorname{Re}(s)=c} x^{-s}\,\Gamma(s)\, ds,$$

la droite $\operatorname{Re}(s) = c$ étant orientée dans le sens des ordonnées croissantes. (Cette convention d'orientation est conservée pour toutes les intégrales analogues apparaissant dans le problème.)

Si z est un nombre complexe non nul, on note $\operatorname{Arg}(z)$ l'unique détermination de l'argument de z qui appartient à $[-\pi, \pi[$, et l'on pose $\operatorname{Log}(z) = \operatorname{Log}|z| + i\operatorname{Arg}(z)$, puis, pour tout nombre complexe a, $z^a = e^{a \operatorname{Log}(z)}$.

Dans tout le problème, $\mathscr{P}$ désigne l'ensemble des nombres complexes dont la partie imaginaire est strictement positive.

Soit λ un réel strictement positif; une fonction f définie dans $\mathscr{P}$ est dite périodique, de période λ, si, quel que soit $z \in \mathscr{P}$, on a $f(z + \lambda) = f(z)$.

PREMIÈRE PARTIE.

I. — 1° Soit f une fonction définie dans $\mathscr{P}$, holomorphe et périodique de période λ.

a) Démontrer qu'il existe une fonction g, définie et holomorphe dans l'ouvert

$$\{z \mid z \in \mathbf{C} \quad \text{et} \quad 0 < |z| < 1\},$$

telle que

$$g(e^{2i\pi z/\lambda}) = f(z).$$